Ekonomiczne Problemy Usług nr 2/2018 (131), t. 1

ISSN: 1896-382X | www.wnus.edu.pl/epu
DOI: 10.18276/EPU.2018.131/1-18 | strony: 183–191

Krzysztof Kubiak
Politechnika Poznańska
Katedra Marketingu i Sterowania Ekonomicznego
krzysztof.kubiak@put.poznan.pl

Bartosz Kardasz
Politechnika Poznańska
Wydział Inżynierii Zarządzania
bartosz.kardasz@gmail.com

Sposoby ochrony wiedzy w przedsiębiorstwie sektora high-tech – *case study*

Kody JEL: L21, L26
Słowa kluczowe: ochrona wiedzy, wiedza chroniona, sektor high-tech
Streszczenie. We współczesnym przedsiębiorstwie zasób, który ma gwarantować uzyskanie przewagi konkurencyjnej, powinien podlegać ochronie. Ochrona dotyczy nie tylko zagrożeń zewnętrznych, ale również wewnętrznych, losowych oraz intencjonalnych. W celu określenia właściwej ochrony wiedzy w przedsiębiorstwie istotne jest jej zidentyfikowanie, w tym określenie poziomu akceptowalności ryzyka. Formalizacja procedur sprawia, że wiedza i umiejętności pracowników przechowywane w umysłach pracowników są rejestrowane i stają się własnością firmy. Przedsiębiorstwa wysokich technologii, nazywane również jako high-tech, samodzielnie wytwarzają oraz intensywnie wykorzystują własną niepowtarzalną wiedzę w różnych obszarach, dostarczając na rynek innowacyjne rozwiązania, takie jak nowe generacje wyrobów czy stosowane technologie produkcji. W tym aspekcie szczególna powinna być ochrona samodzielnie wytworzonej i niepowtarzalnej wiedzy. Celem artykułu jest identyfikacja wybranych sposobów ochrony wiedzy w przedsiębiorstwie sektora high-tech, który to jest „lokomotywą" rozwoju gospodarczego.

Wprowadzenie

Kapitał intelektualny organizacji jest istotnym czynnikiem decydującym o jej dynamicznym rozwoju. Jednym z jego istotnych czynników jest zasób wiedzy, który powinien podlegać ochronie. Gwałtowny wzrost zapotrzebowania na wiedzę, a także

możliwości dostępu do niej, wymagają ciągłego poszukiwania i wykorzystywania odpowiednich sposobów jej selekcji, wyboru i przyswajania. We wszystkich etapach procesów innowacyjnych, począwszy od badań naukowych, przez prace badawczo-rozwojowe (bez działalności B+R gospodarka oparta na wiedzy nie będzie się jednolicie rozwijać) (Budziewicz-Guźlecka, 2014, s. 8), po procesy dyfuzyjne i wdrożeniowe, tworzona jest własna i wykorzystywana obca wiedza. Z tego powodu powstają wciąż nowe, nieustannie rozwijające się w skali międzynarodowej różnorodne rozwiązania, które są niezbędne do tego, by dana wiedza należała do określonych podmiotów, którym przysługują wyłącznie prawa do jej korzystania w określonym czasie, ale także na wyznaczonym terenie (Kozłowski, 1995, s. 17).

Liczba wynalazków z roku na rok wzrasta, w związku z tym coraz więcej osób i instytucji ubiega się o ochronę swoich patentów. Ochronie podlegają coraz większa ilość utworów, zarówno naukowych, gospodarczych oraz badawczych, w tym także znajdują się publikacje naukowe, programy komputerowe, opracowania, raporty, ale także bazy danych i dokumentacje.

Niewątpliwie ochrona własności prywatnej wpływa na wzrost innowacji, a te z kolei stanowią o rosnącym tempie wzrostu gospodarczego (Bochańczyk-Kupka, 2017, s. 162).

Współcześnie sukces gospodarczy jest mierzony nie tylko udziałem firmy na rynku, ale również procesem zarządzania wiedzą oraz umiejętnością wykorzystania kapitału intelektualnego (Grudzewski, Hejduk, 2004, s. 133).

W sytuacji, gdy mamy do czynienia z dużą konkurencyjnością rynków, dostrzegamy, iż charakteryzują się one dynamiką zmian, ponieważ różnego rodzaju technologie można zakupić, natomiast określone modele biznesowe da się skopiować. Zarządzanie wiedzą ułatwiło zatem znalezienie odpowiedzi na pytanie, gdzie należy szukać źródeł wartości przedsiębiorstw. Istotna jest zatem wiedza chroniona, która jest zasobem decydującym o uzyskaniu przewagi konkurencyjnej firmy na rynku. Celem artykułu jest identyfikacja wybranych sposobów ochrony wiedzy w przedsiębiorstwie sektora high-tech. Do realizacji tego celu zastosowano metodę *case study*. W części badawczej wykorzystano obserwację uczestniczącą, analizę dokumentacji wewnętrznej i zewnętrznej przedsiębiorstwa, w tym procedury dotyczące ochrony wiedzy.

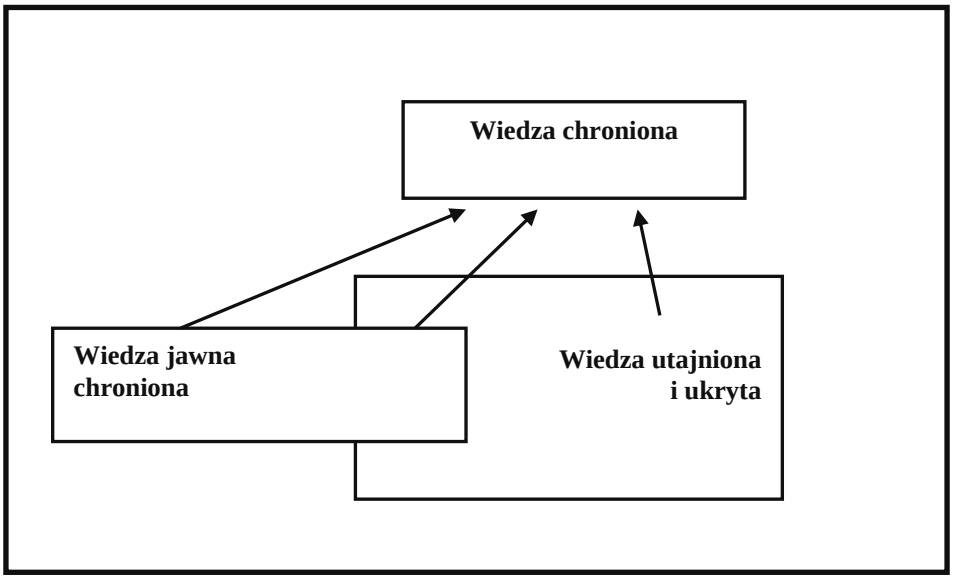
1. Istota wiedzy chronionej

Jednym z wyzwań w zarządzaniu wiedzą jest zapewnienie jej bezpieczeństwa. W tym zakresie istotne są: właściwa eksploracja danych, odpowiednie systemy multimedialne czy też systemy danych sieciowych. Ponadto należy chronić aktywa przedsiębiorstwa, takie jak własność intelektualna. Oznacza to, że należy egzekwować pewne formy kontroli dostępu, np. kontrola oparta na rolach, mechanizm poświadczeń oraz szyfrowanie (Bertino, 2006, s. 429).

Każda wiedza, która ma być poddana ochronie prawnej, musi charakteryzować się wysokim poziomem konkurencyjności. Najistotniejszym kryterium podziału wiedzy chronionej jest przede wszystkim jej dostępność, co oznacza możliwość swobodnego jej wykorzystywania. Zgodnie z tą klasyfikacją wyróżnia się trzy podstawowe kategorie wiedzy (Kotarba, 2005, s. 9):

- wiedzę wolną, która w pełni jest dostępna,
- wiedzę jawną chronioną,
- wiedzę niedostępną, która jest utajniona lub ukryta.

Terminologia wiedzy chronionej zawiera czystą postać wiedzy jawnie chronionej, ale także wiedzy utajnionej. Ponadto może również składać się z kombinacji powyższych rodzajów wiedzy (Kotarba, 2005, s. 10) (rys. 1).

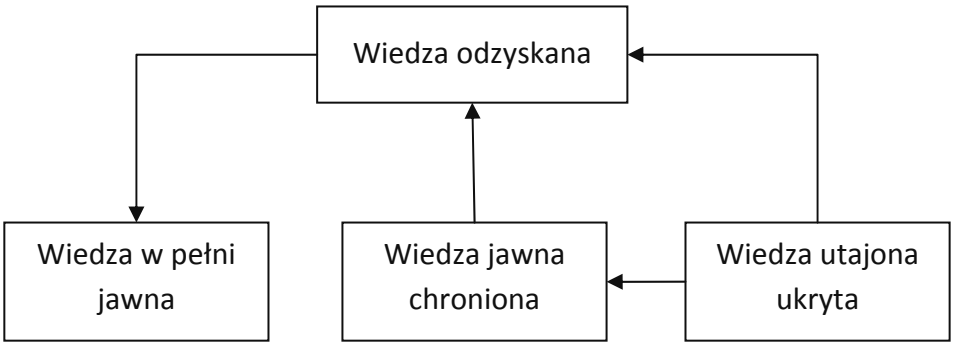


Rysunek 1. Rodzaje wiedzy chronionej wykorzystywane w organizacji

Źródło: Kotarba (2005), s. 10.

Wiedza chroniona to wszystkie wytwory umysłu ludzkiego, które istnieją w sensie prawnym, a także majątkowym, bez względu na produkty czy usługi, których dotyczą. Pod względem praktycznym organizacje są w stanie wykorzystywać wiedzę chronioną na trzy sposoby: „wyłącznie wiedzę jawną chronioną, wyłącznie wiedzę utajnioną, a najczęściej również jawną chronioną i utajnioną" (Kotarba, 2005, s. 9). Najczęstszym rozwiązaniem w postaci chronionego patentem wynalazku współtowarzyszy wiedza utajniona w postaci know-how. Zarówno wiedza jawna chroniona, jak i wiedza utajniona, z upływem czasu przeobrażają się w wiedzę wolną, jednak wiedza utajniona ma prawo przekształcić się w wiedzę jawną chronioną zanim jeszcze stanie się wiedzą

jawną. Natomiast odzyskaną nazwiemy wiedzę chronioną przekształconą w wiedzę wolną (Kotarba, 2005, s. 11) (rys. 2).



Rysunek 2. Przekształcanie wiedzy

Źródło: opracowanie własne na podstawie Kotarba (2005).

Ochrona informacji i wiedzy organizacyjnej powinna obejmować następujące obszary (Materska, 2005, s. 17):

- kontrolę pozyskiwania, wytwarzania i przetwarzania informacji i wiedzy,
- bezpieczną dystrybucję omawianych zasobów,
- monitorowanie „dróg" informacji i wiedzy w strukturze danej organizacji,
- szkolenie personelu w zakresie procedur bezpieczeństwa.

Według Probsta, Rauba i Romharda (2002, s. 184) ochrona wiedzy ma ustrzec organizację przed utratą tego cennego zasobu oraz nieuprawnionym wykorzystaniem jej doświadczeń i informacji przez konkurentów. Wzrost świadomości w zakresie ochrony wiedzy wymaga uruchomienia procesu jej identyfikacji, zbudowania architektury strategicznej i programowania celów firmy, określenia parametrów wzrostu, priorytetów rozwoju nowych działalności, wypracowania jasnego sposobu alokacji zasobów zasilających procesy tworzenia wiedzy (Sołek, 2012, s. 93).

2. Charakterystyka badanego przedsiębiorstwa high-tech

Internet oddziałuje na wszystkie obszary gospodarki, w tym także na działania w obszarze high-tech (Drab-Kurowska, 2011). Do sektora high-tech można zaliczyć przemysł informatyczny i komunikacyjny ICT, przemysł farmaceutyczny, lotniczy, optyczny, biotechnologię, nanotechnologię. W Polsce największe firmy high-tech to przede wszystkim zagraniczne korporacje światowe. W części z nich prace w obszarze B+R czynione są w krajach macierzystych, a w Polsce ma miejsce jedynie produkcja. Przedsiębiorstwa high-tech samodzielnie wytwarzają i intensywnie wykorzystują wła-

sną, niepowtarzalną wiedzę w obszarze technicznym, technologicznym i organizacyjnym (Kubiak, 2011, s. 31). W tym zakresie szczególna jest jej ochrona.

Analizowane przedsiębiorstwo oferuje doradztwo finansowe dla klientów indywidualnych, instytucjonalnych i korporacyjnych na całym świecie, ale także dla klientów prywatnych w Szwajcarii. Struktura operacyjna Grupy obejmuje: Centrum Korporacyjne i pięć pionów biznesowych: Zarządzanie Własnością, Zarządzanie Bogactwem Ameryki, Bankowość Personalną i Korporacyjną, Zarządzanie Aktywami i Bank Inwestycyjny. Wszystkie podmioty są efektywne pod względem kapitałowym i korzystają z silnej pozycji konkurencyjnej na swoich rynkach docelowych.

Główna siedziba firmy mieści się w Zurychu w Szwajcarii. Ponadto firma jest obecna we wszystkich największych centrach finansowych na całym świecie. Przedsiębiorstwa posiada oddziały w 52 krajach, a około 34% pracowników zatrudnionych jest w obu Amerykach, 34% w Szwajcarii, 18% w pozostałej części Europy, na Bliskim Wschodzie i w Afryce oraz 14% w regionie Azji i Pacyfiku. W rezultacie firma zatrudnia około 60 000 osób na całym świecie.

Priorytetem firmy jest ciągłe doskonalenie i zwiększanie swoich możliwości w zakresie nowych technologii i digitalizacji, koncentrując się głównie na innowacyjnych rozwiązaniach, mających wpływ na lepszą obsługę klientów i na wzmacnianie pozycji konkurencyjnej na rynku.

3. Ochrona wiedzy w wybranym przedsiębiorstwie high-tech

Analizowane przedsiębiorstwo, działając w wielu krajach i posiadając dużą liczbę pracowników, musi liczyć się z ryzykiem, że ich wiedza może przedostać się do konkurencji. Aby temu zapobiec, wprowadzono kilka zasad, które muszą być bezwzględnie przestrzegane przez wszystkich pracowników.

Biorąc pod uwagę aspekt prawny przedsiębiorstwa, każdy pracownik, wykorzystujący w swojej codziennej pracy i mający dostęp do danych wrażliwych, jest zobowiązany do przestrzegania zasad poufności udostępnianych mu informacji. Zasady są sprecyzowane w dokumentach dostępnych na portalu firmowym oraz wdrażane w formie obowiązkowych szkoleń i egzaminów dla każdego pracownika. Ponadto, każda informacja przed wysłaniem zostaje sklasyfikowana, czy jej treść nie narusza zasad poufności danych. Wiadomości przesyłane między pracownikami lub wychodzące na zewnątrz są monitorowane przez dział informatyczny. Pracownik zgadza się ich przestrzegać, podpisując umowę o pracę. Odpowiednia klauzula w umowie zawartej między pracownikiem a pracodawcą opisuje obowiązki oraz kary wobec pracownika w przypadku ich nieprzestrzegania.

Zasady zdefiniowane przez firmę dotyczą również jej partnerów biznesowych oraz dostawców systemów informatycznych, którzy w celu implementacji oprogramowania muszą mieć dostęp do danych wrażliwych. Dlatego też każdy partner biznesowy jest dokładnie weryfikowany. W pierwszej fazie wdrażane są procedury weryfikacyjne

nowego partnera oraz prowadzony jest wewnętrzny ranking pod względem zaufania do partnera biznesowego, ale także jego ważności pod względem strategicznym. Kluczowe projekty powierzane są tylko i wyłącznie zaufanym, sprawdzonym partnerom, w stosunku do których nie istnieje prawdopodobieństwo wypływu lub też kradzieży danych. Niemniej jednak nawet jeśli nowy partner biznesowy zostanie zaproszony do realizacji kluczowych projektów, powinien współpracować z osobą z wewnętrznej struktury firmy z wyższego szczebla, która będzie monitorować wszystkie jego działania.

Każde oprogramowanie musi być dokładnie przetestowane oraz zatwierdzone przez społeczność ekspertów z danej dziedziny. Pracownik może zgłosić dany produkt, program lub pewne usprawnienie do zatwierdzenia. Jednakże proces ten jest długotrwały.

Zgodnie z podpisaną przez pracowników klauzulą, każdy produkt czy też usprawnienie wytworzone przez pracownika jest własnością firmy. Pracownik, podpisując umowę, zrzeka się praw autorskich na rzecz podmiotu gospodarczego. Niemniej jednak jest to standardowa procedura w przypadku wytwarzania oprogramowania i jest często wykorzystywana przez firmy z sektora high-tech. Pracownicy, którzy nie przestrzegają zasad bezpieczeństwa informacji, zostają przez przedsiębiorstwo zwolnieni.

Do kolejnych rozwiązań informatycznych, które służą zabezpieczeniu wiedzy i informacji chronionych w firmie należą:

- monitorowanie ruchu sieciowego wewnątrz firmy i informacji wypływających drogą elektroniczną na zewnątrz firmy,
- dostęp tylko do oprogramowania zatwierdzonego przez firmę, szkolenia personelu w zakresie procedur bezpieczeństwa,
- dostęp tylko do stron internetowych zatwierdzonych przez firmę,
- system uprawnień pozwalający na przeglądanie zasobów tylko i wyłącznie po otrzymaniu autoryzacji przez przełożonego,
- przydzielone uprawnienia są weryfikowane regularnie przez odpowiedni dział,
- szkolenia i egzaminy, mające na celu wdrożenia wiedzy na temat przechowywania dokumentów oraz przeciwdziałaniu zachowań niepożądanych (tzw. *whistleblowing*),
- dostęp/logowanie do systemów firmy tylko i wyłącznie poprzez autoryzację odpowiednią kartą dostępu oraz hasłem,
- dostęp do budynku tylko i wyłącznie poprzez autoryzację odpowiednią kartą dostępu.

W tabeli 1 przedstawiono zestawienie wykorzystywanych narzędzi i rozwiązań przez badane przedsiębiorstwo z sektora high-tech z podziałem na obszar poddany ochronie oraz na ich skuteczność.

Tabela 1. Wykorzystywane narzędzia i rozwiązania w przedsiębiorstwie high-tech z podziałem na obszar ochrony wiedzy oraz skuteczność ochrony wiedzy

Obszar podlegający ochronie	**Wykorzystywane narzędzia /rozwiązania**	**Skuteczność**
Pozyskiwanie, wytwarzanie i przetwarzanie wiedzy oraz informacji	klauzula podpisywana przez każdego pracownika	niska
	testowanie i zatwierdzanie wykorzystywanego oprogramowania przez ekspertów	średnia
	dostęp tylko do stron internetowych zatwierdzonych przez firmę	średnia
	system uprawnień pozwalający na przeglądanie zasobów tylko i wyłącznie po otrzymaniu autoryzacji przez przełożonego	wysoka
	regularna weryfikacja uprawnień	wysoka
Dystrybucja wiedzy	weryfikacja partnerów biznesowych	średnia
	kluczowe projekty przydzielane są tylko zaufanym biznes partnerom	średnia
	dostęp do budynku tylko poprzez autoryzację kartą dostępu	średnia
	dostęp do systemów firmy tylko poprzez autoryzację odpowiednią kartą dostepu oraz hasłem	wysoka
Monitorowanie „dróg" informacji i wiedzy w strukturze firmy	monitorowanie ruchu sieciowego wewnątrz firmy jak i informacji wypływających drogą elektroniczną na zewnątrz firmy	wysoka
Szkolenia pracowników	szkolenia i egzaminy dotyczące przechowywania oraz przesyłnia dokumentów	średnia

Źródło: opracowanie własne.

Zaproponowane rozwiązania dotyczą sposobów ochrony wiedzy poprzez rozwiązania proceduralne oraz informatyczne. Niewątpliwie głównym nośnikiem wiedzy jest człowiek i to od niego zależy jej bezpieczeństwo.

Podsumowanie

Rozwój przedsiębiorstw wysokich technologii jest jednym z głównych czynników rozwoju gospodarki opartej na wiedzy. Przedsiębiorstwa te ponoszą ryzyko najnowszych rozwiązań technicznych, bardzo często są także wytwórcami nowej i niepowtarzalnej wiedzy. W związku z tym muszą dążyć do zapewnienia należytego poziomu bezpieczeństwa, szczególnie w zakresie jej ochrony. Co za tym idzie, w każdej organizacji powinien funkcjonować prawidłowo przebiegający proces selekcji i ochrony wiedzy, w którym zminimalizowane będą czynniki generujące ryzyko. Badane przedsiębiorstwo sektora high-tech chroni własną i niepowtarzalną wiedzę i tym samym znacząco minimalizuje ryzyko niepożądanego jej wykorzystania. Firma również implementuje nowe rozwiązania, mogące przyczynić do zwiększonej ochrony wiedzy. Analizowane przedsiębiorstwo planuje wdrożyć nowe rozwiązania informatyczne w celu lepszej kontroli przepływu danych między pracownikami wewnątrz firmy, ale również, aby zapobiec niepożądanemu wypływowi wiedzy chronionej poza struktury organizacji.

Literatura

Bertino, E, Khan, L.R., Sandhu, R., Thuraisingham, B. (2006). Secure Knowledge Management: Confidentiality, Trust and Privacy. *IEEE Transactions on Systems Man, and Cybernetics*, *36* (3).

Bochańczyk-Kupka, D. (2017). Państwo a ochrona własności intelektualnej. *Zeszyty Naukowe Uniwersytetu Ekonomicznego w Katowicach. Studia Ekonomiczne*, *311*.

Budziewicz-Guźlecka, A. (2014). Rola działalności naukowo-badawczej w rozwoju gospodarki opartej na wiedzy. *Zeszyty Naukowe Uniwersytetu Szczecińskiego. Ekonomiczne Problemy Usług*, *112*, 9–17.

Drab-Kurowska, A. (2011). Wykorzystanie technologii informatycznych w komunikacji marketingowej. *Zeszyty Naukowe Uniwersytetu Szczecińskiego. Ekonomiczne Problemy Usług*, *68*, 674–681.

Grudzewski, W.M., Hejduk, I.K. (2004). *Zarządzanie wiedzą w przedsiębiorstwie*. Warszawa: Difin.

Kotarba, W. (2005). *Ochrona wiedzy w Polsce*. Warszawa: Orgmasz.

Kozłowski, J. (1995). *Polityka naukowa – polityka innowacyjna*. Warszawa: KBN.

Kubiak, K. (2011). Transfer wiedzy w koncernach high-tech. W: M.K. Wyrwicka (red.), *Sieci gospodarcze Wielkopolski – scenariusze transformacji wiedzy wspierające innowacyjną gospodarkę*. Poznań: Wydawnictwo Politechniki Poznańskiej.

Materska, K. (2005). *Rozwój koncepcji informacji i wiedzy jako zasobu organizacji*. Pobrano z: bbc.uw.edu.pl (15.01.2018).

Probst, G., Raub, S., Romhardt, K. (2002). *Zarządzanie wiedzą w organizacji*. Kraków: Oficyna Ekonomiczna.

Sołek, C. (2012). Dzielenie się wiedzą i ochrona wiedzy w przedsiębiorstwie. *Zeszyty Naukowe Politechniki Rzeszowskiej. Zarządzanie i Marketing, 3*.

VARIOUS MANNERS OF KNOWLEDGE PROTECTION IN HIGH-TECH SECTOR – CASE STUDY

Keywords: knowledge protection, protected knowledge, high-tech sector

Summary. The resources which guarantee gaining competitive advantage should be under protection in contemporary enterprises. The protection concerns not only external hazards and but also internal, accidental and intentional ones. In order to elaborate suitable knowledge protection in an enterprise, it is essential to identify its extent, which includes assessment of acceptable risk. Due to formalization of procedures in an enterprise, knowledge and skills of its employees are registered and become its property. High-technology enterprises, also known as high-tech, produce independently and make an intensive use of their own unique knowledge in various fields, bringing innovative solutions, such as new generations of products or applied manufacturing technologies, onto the market. Taking this aspect into consideration, independently produced and unique knowledge should be under special protection. The purpose of this article is to identify chosen manners of knowledge protection in an enterprise operating in a high-tech sector, which is an "engine" of economic growth.

Translated by Krzysztof Kubiak

Cytowanie

Kubiak, K., Kardasz, B. (2018). Sposoby ochrony wiedzy w przedsiębiorstwie sektora high-tech – case study. *Ekonomiczne Problemy Usług*, 2 (131/1), 183–191. DOI: 10.18276/epu.2018.131/1-18.